FUJ00232604

Fujitsu Services RMGA Information Security Management System (ISMS) Manual
Commercial in Confidence

Document Title:	Fujitsu Services RMGA Information Security Management System (ISMS) Manual
Document Reference:	SVM/SEC/MAN/0003
Document Type:	MANUAL
Release:	Not Applicable
Abstract:	An approach and framework to implementing, maintaining, monitoring and improving information security on the RMG Account
Document Status:	APPROVED
Author & Dept:	Neneh Lowther
External Distribution:	Sue Lowther

Approval Authorities:

Name	Role	Signature	Date
Wendy Warham	Operations Director		
Howard Pritchard	Chief Information Security Officer		

Note: See Royal Mail Group Account HNG-X Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.

FUJ00232604

0 Document Control

0.1 Table of Contents

0 DOCUMENT CONTROL 4
0.1 Review Details 4
0.2 Associated Documents (Internal & External) 4
0.3 Abbreviations 6
0.4 Glossary 6
0.5 Changes Expected 6
0.6 Copyright 7
1 INTRODUCTION 8
2 ISMS OBJECTIVES 9
3 SCOPE OF THE FUJITSU SERVICES RMGA ISMS 10
3.1 Fujitsu Group Security 10
3.2 Fujitsu Corporate Information Systems 10
3.3 Infrastructure Services 10
4 RISK MANAGEMENT 10
4.1 Methodology and Tool 11
4.2 Risk Assessment 11
4.3 Risk Treatment Plan 12
5 ISMS STRUCTURE FOR RMG ACCOUNT 12
5.1 Statement of Applicability 13
5.2 Document and Record Management 13
6 COMPLIANCE AND REPORTING 14
6.1 ISO27001 Compliance Audits 14
6.2 Reporting 15
6.3 Supporting Post Office Ltd Compliance 15
7 COMMUNICATION AND AWARENESS 15
8 OPERATIONAL SECURITY 15
8.1 User Administration 15
8.2 Administration of Changes 16
8.3 Acceptance into Service 16
8.4 Analyse Security Logs 16
8.5 Anti-Virus and Malicious Software Management 17
8.6 Security Incident Reporting and Problem Management 17
8.7 Cryptographic Key Management 17

FUJ00232604

8.8 Information Retrieval and Prosecution Support....18
8.9 Physical Access Control....18
8.10 Subject Information Requests Management....18

9 ORGANISATION....19

9.1 Internal Fujitsu Responsibilities....19
9.2 Fujitsu Services RMG Account Director....19
9.3 Fujitsu Services RMGA Programme Director....19
9.3.1 Fujitsu Services Audit Manager....19
9.4 Fujitsu Services RMGA Operations Director....20
9.5 Chief Information Security Officer (CISO)....20
9.6 Staff Responsibilities....20
9.6.1 Electronic Mail....21
9.7 External Interfaces....21
9.7.1 External Third Parties....21
9.8 RMGA Information Security Management Review (ISMR)....21

FUJ00232604

0.2 Document Control

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1		Initial Draft	
0.2	19/02/08	Updated with information from service description	
0.2	19/02/08	Issued for Review	
1.0	30/04/08	Issued for Approval after updating with review comments	

0.3 Review Details

Review Comments by :	30th March 08
Review Comments to :	Neneh.Lowther GRO & RMGADocumentManagement GRO
Mandatory Review	
*Chief Information Security Officer (CISO)	Howard Pritchard
*RMGA Operational Security Manager	Pete Sewell
*RMGA Information Governance	Brian Pinder
*Service Delivery Manager	Richard Brunskill
Optional Review	
Operations Director	Wendy Warham
Programme Assurance Manager	Jan Holmes
Issued for Information – Please restrict this distribution list to a minimum	
Head of Information Security, POL	Sue Lowther
RMGA Operational Security Manager	Pete Sewell
RMGA Information Governance	Brian Pinder

(*) = Reviewers that returned comments

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	2.0	16-Apr-07	RMGA HNG-X Generic Master Document Template	Dimensions
SVM/SDM/POL/0035	0.2		RMGA INFORMATION SECURITY MANAGEMENT REVIEW (ISMR)	Dimensions
PGMPASMAN0004			BMS Implementation Approach	Dimensions
SVM/SEC/MAN/0003	0.2		ISMS Manual	Dimensions

FUJ00232604

SVM/SEC/MAN/0002	0.2		Information Security Management System (ISMS) Scope	Dimensions
SVM/SEC/STD/0006	1.0		Information Risk Management Approach	Dimensions
SVM/SEC/PLA/0001	0.1	02/04/08	Information Security Risk Treatment Plan	Dimensions
SVM/SEC/STD/0007			Security Control Framework	Dimensions
SVM/SEC/MAN/0001			Statement of Applicability	Dimensions
SVM/SEC/STD/0027			FS RMGA ISMR Terms of Reference	Dimensions
SVM/SEC/STG/0001			Information Security Communications Strategy	Dimensions
SVM/SEC/POL/0003	0.4		RMGA Information Security Policy	Dimensions
ITS/8			Electronic Mail	Dimensions
RS/PRO/048			Horizon Patch Management Process for Operational Security	Dimensions
RS/PRO/049			Horizon Event Logging Process for Operational Security	Dimensions
			SCM Process for Handling AV Process	Dimensions
IA/PRO/004	3.0		Audit Data Extraction	PVCS
NB/PRO/003	2.0		Network Banking Management of Prosecution Support	PVCS
RS/PRO/013	6.0		Horizon Security Pass	PVCS
CS/SER/016			Security Management Service Description. (Current). Commencement of HNG-X Project, Workstream X4 (HNG-X Application Rollout), this document will be replaced by Security Management Service: Service Description (SVM/SDM/SD/0017)	PVCS
CSPRO179			Moneygram Password Procedure	Dimensions
SVMSDMPRO0018			Incident Management Process	Dimensions
CSPRO109			Subject Access Requests	Dimensions
CSPRO040			Live Access Request	Dimensions
CSPLA102			Disaster Recovery Plan	Dimensions
DSMAN002			Signing Server User Guide	Dimensions
RSPRO002			Horizon Vetting Process	Dimensions
RSMAN006			KMS User Guide	Dimensions

FUJ00232604

SVMSDMPRP0018			RMGA Customer Service Incident Management Process	Dimensions
SVMSDMPRO0025			RMGA Customer Service Problem Management Process	Dimensions
SVM/SEC/PLA/004	1	16/04/08	Risk Treatment Matrix	Dimensions
SVM/SEC/PLA/005	1	16/04/08	Security Improvement Matrix	Dimensions
RS/PRO/016	3	12/12/05	Physical Access to Post Office Sites	PVCS
QU/DOC/002	3	03/06/05	Security Awareness Leaflet	PVCS
SVM/SEC/STD/0026			CISO TOR	Dimensions

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

0.5 Abbreviations

Abbreviation	Definition
IG	Information Governance
ISMR	Information Security Management Review
ISMS	Information Security Management System
NCN	Non-Conformity Notice
RMGA	Royal Mail Group Account
ToR	Terms of Reference
Fujitsu	Fujitsu Services RMG Account,
CISO	Chief Information Security Officer
RTP	Risk Treatment Plan
ISP	Information Security Policy
SOA	Statement of Applicability
ARQ	Audit Request Query
SLA	Service Level Agreement
OLA	Operational Level Agreement

0.6 Glossary

Term	Definition

0.7 Changes Expected

Changes

FUJ00232604

0.8 Copyright

FUJ00232604

1 Introduction

Best practice, as defined in ISO/IEC 27001:2005, BS 7799-2:2005 requires an approach and framework to implementing, maintaining, monitoring and improving information security. This document provides a high level overview of the approach and framework, known as the Information Security Management System, used within the Fujitsu Services RMGA and will be independently reviewed on at least an annual basis. The document is structured to explain the Security Management framework and is supported by the following key documents:

Key Information Governance Documents	Key Operational Security Documents
SVM/SEC/MAN/0003 ISMS Manual (this document)	RS/PRO/048 Horizon Patch Management Process for Operational Security
SVM/SEC/MAN/0002 Information Security Management System (ISMS) Scope	RS/PRO/049 Horizon Event Logging Process for Operational Security
SVM/SEC/STD/0006 Information Risk Management Approach	SCM Process for Handling AV Process
SVM/SEC/PLA/0001 Information Security Risk Treatment Plan	IA/PRO/004 - Audit Data Extraction
Security Control Framework	NB/PRO/003 - Network Banking Management of Prosecution Support
SVM/SEC/MAN/0001 Statement of Applicability	RS/PRO/013 - Horizon Security Pass Procedure
SVM/SEC/STD/0027 FS RMGA ISMR Terms of Reference	Security Management Service Description. (Current). Commencement of HNG-X Project, Workstream X4 (HNG-X Application Rollout), this document will be replaced by Security Management Service: Service Description (SVM/SDM/SD/0017)
SVM/SEC/STG/0001 Information Security Communications Strategy	CSPRO179 Moneygram Password Procedure
SVM/SEC/POL/0003 RMGA Information Security Policy	SVMSDMPRO0018 Incident Management Process
ITS/8 Electronic Mail	
SVM/SEC/STD/0026 CISO TOR	CSPRO109 Subject Access Requests
	CSPRO040 Live Access Request
	CSPLA102 Disaster Recovery Plan
	DSMAN002 Signing Server User Guide
	RSPRO002 Horizon Vetting Process

FUJ00232604

	RSMAN006 KMS User Guide
	SVM/SDM/SD/0017 Security Service Description

2 ISMS Objectives

The objectives of the ISMS are to:

- Provide a security framework within which the Service is developed, implemented and delivered by Fujitsu in all areas of its business and responsibilities as required under Schedules A4:4.1.2 of the Agreement which states that 'Fujitsu services shall be in compliant with ISO 27001'.
- Provide an organisational and responsibility framework for security activities within Fujitsu and allocate security roles and responsibilities
- Identify risks associated with the provision of the Service, through formal risk assessment techniques, and prioritise and implement appropriate controls and security measures
- Ensure appropriate security and business continuity procedures and controls are in place to support Services provided by Fujitsu
- Provide a basis for review, governance, assessment and improvement of the ISMS
- Ensure that information security controls are appropriate to the sensitivity of the information processed and stored
- Identify the security awareness and education requirements for all Fujitsu RMGA employees and subcontractors
- Describe the compliance, audit and management arrangements

3 Scope of the Fujitsu Services RMGA ISMS

The Fujitsu Services RMGA ISMS encompasses all aspects of the Fujitsu Services RMGA business and operations in support of discharging Service obligations as defined in the Agreement.

This ISMS is a subset of the RMGA Business Management System (BMS) as described in the BMS Implementation Approach (PGMPASMAN0004)

This includes the design, development, testing, deployment, operation, maintenance, decommissioning and Services transfer of all aspects of the Services provided to Post Office Limited as well as the associated supporting Fujitsu Services RMGA business processes.

A distinct part of the scope of this ISMS is subject to ISO27001 registration, specifically the design, development, test and deployment processes including the delivery, operation and maintenance of the HNGX Service. The document "ISMS Scope" (SVM/SEC/MAN/0002) describes the full scope of the ISMS subject to registration, in terms of technology, people and process.

3.1 Fujitsu Group Security

The Physical Security of Fujitsu Services sites are provided by Fujitsu Group Security. Any requirements that RMGA has for additional security is requested by the CISO or Operational Security Manager from the Head of Group Security.

Information about incidents affecting the physical security of Fujitsu Services RMGA sites are provided to the Operational Security Manager by Group Security.

FUJ00232604

Group Security also has responsibility for the vetting procedures for Fujitsu Services RMGA staff although local advice and guidance can be obtained from the RMGA operational security team.

3.2 Fujitsu Corporate Information Systems

The information security of Fujitsu Corporate Information Systems is managed by Fujitsu Corporate Information Services and their use is subject to the Fujitsu Services Security Master Policy (CPM/20).

3.3 Infrastructure Services

Infrastructure Services provide some elements of the Services to RMGA and are bound to comply with the RMGA Information Security Policy. However, Infrastructure Services operate their own ISO27001 registered ISMS with which this ISMS interfaces.

4 Risk Management

Fujitsu Services has an approved approach to the management of information security risk for RMGA which is documented in RMGA Information Risk Management Approach.

Fujitsu Services RMGA is required to conduct a robust programme of risk management (incorporating risk identification, assessment and mitigation) as a means of determining and confirming the appropriateness of information related security controls for Programme systems and services. The risk management programme is, on a day-to-day basis, undertaken by the Fujitsu Services RMGA IG staff. Although the options for risk management (i.e. acceptance, transfer, mitigation etc) are determined by the IG staff and the decision taken by the appropriate Programme or Operational management team, security risk oversight lies with the Information Security Management Review Body (ISMR) , which is the highest authority within the Fujitsu Services RMGA for the management of information security risks. Further information about the ISMR is contained later in this document.

4.1 Methodology and Tool

Fujitsu Services RMGA employs a repeatable risk based approach comprising:

- the identification of key assets and service components;
- the threats they may be subject to;
- an assessment of the range of impacts upon the systems and service, and;
- the recommendation of proposed controls or countermeasures, aimed at;
- allowing management to make appropriate decisions on risk management, by selecting the most relevant control options

The risk assessment methodology and software tool, FRAMES (Version 0.9) is the preferred approach for the assessment of information security risks for RMGA. *FRAMES* is a risk assessment tool based on the ISF SPRINT Methodology, developed in Microsoft Access. It has been designed to carry out Assessments of Risks associated with Information Assets, ranging from applications to data centres. It is intended to be used in a workshop environment where participants can identify impacts, threats, and any necessary controls.

4.2 Risk Assessment

FUJ00232604

Risk assessment and management is not a one-off exercise, with a single set of control recommendations which remain static in time. In the ongoing processes concerned with Programme releases, operational delivery and maintenance of the live service, there will be a number of instances where information risk assessment activity will be necessary:

- Planned risk assessments – these will be part of the normal routine for ensuring that deployed controls remain relevant to the threat environment in which the systems and service operate, as the prevailing threats and vulnerabilities may change over time. This refresh would fall within the 'Check' phase of the 'Plan – Do – Check – Act' control implementation cycle. It may be necessary therefore to conduct risk assessment activity either at planned intervals (e.g. 6-monthly or annual) to confirm that controls are still relevant, or to carry out a risk review on specific components of the service or infrastructure where assurance as to the continued effectiveness of controls is required.
- Reactive risk assessments – As part of service management, incidents, issues or threat notifications may indicate a need for a reactive review of the potential impact of particular threats or new vulnerabilities. This may be as a result of a single serious incident or as an escalating or cumulative trend. The objective of this review may be to verify if existing controls are sufficient to deal with the new or escalating threats/vulnerabilities, or require strengthening.

4.3 Risk Treatment Plan

In accordance with the dictates of best practice, RMGA maintains a Risk Treatment Plan (RTP) (Information Security Risk Treatment Plan)

Information risks are recorded in the Fujitsu Services RMGA RTP. Risks attracting high probability and impact scores are escalated, as required, through the Fujitsu Services RMGA risk management process (PGM/PAS/MAN/0002)

In addition to regular risk assessments, RTP sources are:

- **ISO/IEC27001 Compliance Rating**
  Each month Fujitsu Services RMGA reports a compliance status, in terms of all ISO27001 control items. Any area with a score of '0' (control not addressed) is recorded in the RTP
- **Audit Non-Conformity Notices (NCN), Observations and Improvements**

  Regular Information Security Policy (ISP) compliance audits are conducted. During the audits, inappropriate controls, or controls improperly implemented, may be identified and, subsequently, an 'NCN', 'Observation' or 'Improvement Opportunity' is raised.

  An 'NCN' is raised where a mandatory control (as defined in the Agreement or ISP) is not addressed or is ineffectively implemented, and this fact is recorded in the RTP.

  An 'Observation' is raised when a recommended control (as defined in the Control Framework) is not effectively implemented

  An 'Improvement Opportunity' record is raised when a control is implemented but there is an opportunity for improvement in the management system
- **Supplementary**

  There are information risks identified by, or notified to, the IG staff and subsequently registered, often as a result of:

  - Specific risk workshops, organised for the purpose
  - Information risks generated by other teams across the account
  - Other compliance and testing activities, which give rise to potential risks requiring mediation

FUJ00232604

- Service incidents which have the potential to cause significant impact, and for which a review of the risk and control position is required

5 ISMS STRUCTURE FOR RMG ACCOUNT

The ISMS is founded on the basic concepts of: Confidentiality; Integrity; Availability. Information Governance staff ensure the co-ordination of all physical protective and logical information security aspects of the premises, facilities, infrastructure and data; and ensure compliance with all Security Controls, and the Security Policy.

However, the ISMS also outlines the management responsibility for ongoing Operational Security of operational Services, including ensuring that the security section in SLAs, OLAs are compliant with, and that Business Continuity plans support the Security Policy and Security Controls. These key operational responsibilities are outlined in section 8.

5.1 Statement of Applicability

Information security is implemented through an appropriate set of controls, which in practice will be a combination of policies, procedures, organisational structures, physical and technical measures.

The selected controls are documented in the Fujitsu Services RMGA Statement of Applicability. Most of the controls are applicable and controls are only excluded where they are outside of the scope or not identified as a risk to the Service delivered to POL.

5.2 Document and Record Management

The RMGA Dimensions system ensures that all documents are readily available from a single source, to the relevant audience.

The Statement of Applicability (SOA) lists all documents relevant to the scope of the ISMS. The SOA can be found in Dimensions.

All documents required by the Fujitsu Services RMGA ISMS are protected and controlled through the RMGA HNG-X Document Control Process (PGM/DCM/PRO/0001). The document process also contains details about document branding, protective marking, document retention and quality templates.

Records are established and maintained to provide evidence of conformity to requirements and the effective operation of the Fujitsu Services RMGA ISMS. The primary records are:

Record	Location	Retention
Risk Assessment Output	Dimensions	7 yrs after termination of the project
Integrated Audit Plan	Dimensions	7 years after termination of the project
Audit Records	Quality Management System	7 years after termination of the project
Security Incident Reporting	Dimensions	7 years after termination of the project

FUJ00232604

System Audit Logs	HNGX Audit Domain.	6 years with a further 1 year of space after termination of the project
Information Security Management Review (ISMR) Minutes	Dimensions	7 years after termination of the project
ISP Reviews	Dimensions	7 years after termination of the project
Risk Treatment Plan	Dimensions	7 years after termination of the project
Information Security Monthly Report	Dimensions	7 years after termination of the project
IG Staff Meeting – Minutes	Dimensions	7 years after termination of the project
Operations Service Acceptance Process –Security Compliance Matrix	Service Management	7 years after termination of the project
Reports of Security Incidents	Secure Area of Dimensions	7 years after termination of the project

6 Compliance and Reporting

6.1 ISO27001 Compliance Audits

In support of the ISO27001 compliance requirements, and to provide ongoing assurance of compliance, regular compliance audits will be conducted. As directed by the Chief Information Security Officer, the scope and terms of reference for each of these audits will be determined in advance and agreed with the manager of the area(s) to be audited.

For each ISO27001 control within the scope of the ISMS the following is reviewed:

- Clear, accepted responsibility for the aspect of Information Security which is subject to that control;
- Confirmation from the organisation that the relevant control is in place, documented and effective;
- Documentary evidence (records/logs etc. in either electronic or hardcopy format), which can be inspected to confirm the controls are in place and functioning as intended. Inspection is on a sampling basis.
- All findings are logged on the Fujitsu Services Assessment Database and updated as action is taken.

All audits will be carried out by suitably trained auditors with auditing qualifications e.g. BS7799/ISO27001 Lead Auditor; TickIT Auditor/Lead Auditor.

Audits are carried out as part of the RMGA Internal Audit Plan (PGM/PAS/PLA/0005). Additional audits are carried out on a regular basis by the FS Manage Information Security Process Champion and Fujitsu Services Business Assurance. As part of ISO27001 registration, independent external audits will be conducted as determined by the audit body.

FUJ00232604

6.2 Reporting

Information Governance staff provide a monthly Information Security Reporting Pack which informs the Management Team, as an input to the Fujitsu Services RMGA ISMR, of progress towards ISO27001 compliance, results of audits and current risk status. It is intended that the details contained in this report will expand over time. This includes reports from the Operational Security Team such as a summary of the types and numbers of incidents that may impact on the confidentiality, integrity or availability of RMGA systems.

A subset of this monthly report is included in the Service Review Book which is provided monthly to the customer.

6.3 Supporting Post Office Ltd Compliance

The RMGA CISO is responsible for assisting POL in achieving information security compliance, by:

- Completing security questionnaires from POL and any of its clients.
- Participating, following a formal written request from POL, in routine audits such as those conducted by POL's Internal Audit team or as part of an overall audit of POL's PCI compliance as referenced in csser016.

7 Communication and Awareness

A programme of security awareness training, including Information Security overviews, is provided to all new arrivals, as part of induction training. The service covers the provision of periodic awareness activities and training including induction training, presentations and briefing notes and input to magazines, journals and other periodicals.

The Fujitsu Services RMGA Security Communications Strategy details the various communication channels that are used and the different vehicles and methods available for ensuring that key messages regarding Information Security are effectively communicated to staff at all levels engaged in the Fujitsu Services RMG Account.

8 Operational Security

8.1 User Administration

The Operational Security Team will be responsible for the administration, issuing and audit of Two Factor authentication used by system administrators and support staff accessing the Live Service.

The Operational Security Team is responsible for ensuring that Fujitsu users of POL Services are validated before being given access to the live Service.

The Operational Security Manager is responsible for ensuring that these tasks are carried out in accordance with the Security Policy and for authorising physical access rights requiring strong authentication for secure access.

8.2 Administration of Changes

Operational Change Management is the responsibility of the Change Management Team within Service Management.

FUJ00232604

The Operational Security Team is responsible for reviewing all change requests and assessing the impact of changes for compliance with Security Policy and Controls and for any impact on the Confidentiality, Integrity and Availability of Services. They are supported in the technical aspects of these assessments by the Technical Security Architects.

8.3 Acceptance into Service

Responsibility for accepting new Services rests with the Service Management Team. The Operational Security team is responsible for ensuring that new services identify their security requirements and that the security elements of Acceptance into Service have been met.

8.4 Analyse Security Logs

The Operational Security team is responsible for providing a number of security event management and firewall event analysis activities:

- Managing and operating the audit mechanisms and security event management system (including firewall events) to monitor, detect, track, record and report events that might threaten the security of the Service Infrastructure (security weaknesses). This includes the review of security event filter to optimise performance;
- Regularly analysing audit trails to identify trends and to assist the investigation of security incidents/breaches;
- Establishing and monitoring adequate firewall policies / rule bases based on the output of risk assessments as appropriate;
- Where potential attacks, or areas of vulnerability, are identified ensuring prompt investigation and providing advice for any remedial action (as part of security incident management) to minimise the impact of any security breach.
- Any successful attacks will be subject to the RMGA Customer Service Incident Management Process.

8.5 Anti-Virus and Malicious Software Management

The Operational Security team provides a number of anti-virus and malicious software management activities. For HNG-X, the updated version of Sophos cover malware as well as anti-virus.

- Managing the distribution of updated anti-virus software across the live estate to protect the Services from malicious software, including regular DAT updates to identify and cleanse new and emerging virus strains;
- Configuring, and maintaining, alerting mechanisms and event filters to provide automatic notification and prompt virus incident response (in accordance with security incident response procedures);
- Regular checking of emerging viruses and other malicious software to determine any required defensive measures;

8.6 Security Incident Reporting and Problem Management

FUJ00232604

The Operational Security Team participate in the RMGA Customer Service Incident Management Process (SVM/SDM/PRO/0018)and RMGA Customer Service Problem Management Process (SVM/SDM/PRO/0025) with regard to Security related Incidents and Problems.

The Operational Security Manager is the prime point of contact for information security related events, incidents and breaches and is responsible for communicating relevant security incident details to POL, as well as attending a joint monthly meeting to review information security incidents.

8.7 Cryptographic Key Management

The Operational Security Team provide a key management service to control the certification and distribution of cryptographic key material used to protect the confidentiality and integrity of Post Office business data. This consists of three primary activities:

- Managing cryptographic key suppliers;
- Manual cryptographic key management – creating, distributing, auditing and replenishment of manual cryptographic keys;
- Managing an automated Key Management System (KMS) - creating, distributing and replenishment of cryptographic material as well as assisting support teams with error resolution and problem management related to the KMS.

The KMS is a critical business system and as such is subject to service optimisation and the provision of business continuity arrangements.

An actual, or suspected, compromise of any keys (including PIN Pads) will be treated as a security incident and managed accordingly. In particular, key change mechanisms will be invoked. If a key is identified compromised a corrective action plan will be carried out in accordance to the agreed correct action response for that key.

An actual, or suspected, compromise of any keys (including PIN Pads) will be treated as a security incident and managed accordingly. In particular, key change mechanisms will be invoked.

8.8 Information Retrieval and Prosecution Support

The operational security team is responsible for the management of the day-to-day extraction of transaction and event data from the audit system, the analysis of supporting information and the provision of associated investigation / prosecution support. This requires close co-operation with Audit and Investigation staff in Post Office Ltd, the provision of witness statements and reports, and possible attendance at Court to give evidence.
Data extracted can be in response to either Transaction Record Queries, or Audit Record Queries, including APOP Voucher Queries (Reference document SVM/SDM/SD/0017).

8.9 Physical Access Control

The Operational Security Team is responsible for the administration, issue and control of the Fujitsu Services (Royal Mail Group Account) Ltd Horizon Security Passes. All staff who require access to a Post Office branch to provide support and maintenance will need to be issued with a Horizon Security

FUJ00232604

Pass. The Horizon Security Pass allows employees of the Royal Mail Group Account (RMGA) to be identified as those who have been successfully vetted by Post Office Limited (POL).

8.10 Subject Information Requests Management

The Operational Security Team is responsible for the management and provision of responses in respect of Subject Information Requests.

9 Organisation

9.1 Internal Fujitsu Responsibilities

Full details of key Fujitsu Services RMGA Security responsibilities are contained within the Information Security Policy. In summary:

9.2 Fujitsu Services RMG Account Director

The information security-related responsibilities of the Fujitsu Services RMG Account Director include:

- Overall control and management of information security throughout the Fujitsu Services RMG Account;
- Provision of adequate resources for information security;
- Appointing an experienced security professional responsible for managing and coordinating security across the complete RMGA domain.
- Approval authority for the Fujitsu Services RMGA Information Security Policy;
- Establishing the information security interface with the customer; and
- Establishing the information security interface with all Fujitsu Services subcontractors

Senior management is supported by the Information Governance staff which consists of experienced specialists with specific expertise in the areas of IT security and risk management.

9.3 Fujitsu Services RMGA Programme Director

The information security-related responsibilities of the Fujitsu Services RMGA Programme Director include:

- Ensuring that responsibilities and procedures for the management and operation of all information processing facilities are established, documented and maintained; and
- Ensuring that changes to information processing facilities and systems are controlled.
- Overall control of risk management and audit functions, including deciding the criteria for accepting risks and the acceptable levels of risk;

9.3.1 Fujitsu Services Audit Manager

FUJ00232604

The information security-related responsibilities of the Fujitsu Services RMGA Programme Assurance Manager include:

- Overall control of risk management and audit functions;
- Co-ordinating all audit related activities;
- Providing a point of contact for external audit personnel;
- Planning and carrying out audits of RMGA's business functions; and
- Maintaining an integrated audit plan

9.4 Fujitsu Services RMGA Operations Director

The information security-related responsibilities of the Fujitsu Services RMGA Operations Director include:

- Sponsorship of the Chief Information Security Officer; (CISO);
- Ownership and overall control and management of operational security throughout RMGA;
- Day to day management of security related risks;
- Chairing the RMGA Information Security Management Review Board; and
- Acting as the approval authority for Royal Mail Group Account's Security Procedures,

9.5 Chief Information Security Officer (CISO)

The CISO is responsible for the overall design of RMGA's security control framework. The CISO will lead the engagement with customer stakeholders with an interest in governance, control and security matters. The CISO will ensure the responsibilities of the Information Governance and Operational Security Teams are met. Full details are contained within the "RMGA CISO Terms of Reference" (Ref SVM/SEC/STD/0026) and include:

- Developing and publishing all security-related policies and guidelines applicable at RMGA level;
- Reviewing and approving information security policies and procedures owned and implemented at business level;
- Providing a point of contact for POL Head of Information Security
- Ensuring that security incidents are recorded and investigated;
- Monitoring for compliance with the RMGA Information Security Policy;
- Ensuring all RMGA Staff are screened in line with contractual requirements, FS Group Policy and this policy;
- Ensuring that security relevant events are recorded
- Ensuring that system audit trails are analysed on a regular basis;
- Defining the information security risk assessment approach of RMGA:
- Analysis and evaluation of information security risks and evaluating options for the treatment of risks; and
- Co-ordinating the implementation and operation of the Information Security Management System.

9.6 Staff Responsibilities

All RMGA Staff have an Information Security related objective to ensure awareness of their security responsibilities and security procedures. Security Induction Training ensures all staff know where to find security procedures, are familiar with their contents, and understand their own responsibilities for compliance.

The information about which staff should be aware includes:

FUJ00232604

- Physical security controls and visitor procedures
- Clear desk policy, careful communications and storage
- Protecting Fujitsu documents and media and protecting RMGA information
- Reporting security incidents
- Responsibilities for the protection of personal data
- Acceptable use of Fujitsu equipment, Internet and email
- Working at home and out of the office

9.6.1 Electronic Mail

Information classified as COMPANY RESTRICTED may be transmitted unencrypted by electronic mail within the Company, providing such mail is flagged as sensitive (e.g. 'Confidential' if sent by Microsoft Exchange/ Outlook). Where transmissions are outside of the company secure approved encryption methods must be used as referenced in (ITS/8 – Electronic Mail).

9.7 External Interfaces

9.7.1 External Third Parties

In accordance with section 6.2.1 of the RMGA Information Security Policy, all services provided by external third parties require a clear contract between Fujitsu Services and the external organisation, detailing all the key aspects of Information Security that are part of the defined service to be delivered, including the right of Fujitsu to audit the security of the service provided.

As with internal support functions, audits will be carried out periodically by Fujitsu to confirm that the various contractual clauses are being adhered to.

In addition Section 10.8 of the RMGA Information Security Policy provides the guidance and controls on the security requirements for exchange of information between third parties.

9.8 RMGA Information Security Management Review (ISMR)

To ensure that areas of security risk or concern are assessed, appropriate controls are defined and effectively implemented and to manage levels of security risk to an appropriate level there is a Management forum, the RMGA Information Security Management Review meeting. Objectives and responsibilities of the meeting are documented in "Fujitsu Services RMGA ISMR Terms of Reference (SVM/SEC/STD/0027)". Also included in the document is a membership list, mode of operation and deliverables.